# Second Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC'16)

Alvaro A. Cárdenas
University of Texas at Dallas
alvaro.cardenas@utdallas.edu

Rakesh B. Bobba
Oregon State University
rakesh.bobba@oregonstate.edu

## ABSTRACT

The Second International Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC'16) is being held in conjunction with the 23rd ACM CCS Conference. This second edition follows a successful workshop held with ACM CCS in 2015. The workshop was motivated by several observations. First, cyber-physical systems represent the new frontier for cyber risk. The attack surface imposed by the convergence of computing, communications and physical control represents unique challenges for security researchers and practitioners. Second, majority of the published literature addressing the security and privacy of CPS reflect a field still in its infancy. As such, the overall principles, models, and theories for securing CPS have not yet emerged. Third, the organizers of this workshop strongly felt that a premiere forum associated with a premiere conference was needed for rapidly publishing diverse, multidisciplinary in-progress work on the security and privacy of CPS and galvanizing the research community. The set of accepted papers reflect this vision. We have organized an exciting program for this workshop and look forward to active participation in this and future workshops.

## Keywords

Cyber-Physical Systems, Security, Privacy, Safety, Reliability

## 1. INTRODUCTION

Cyber-physical systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed by a set of networked agents, including sensors, actuators, control processing units, and communication devices. While some forms of CPS are already in use, the widespread growth of wireless embedded sensors and actuators is creating several new applications in areas such as medical devices, automotive, and smart infrastructure. Equally important is the emergence of Internet of Things (IoT) and how IoT will interface with control systems. As such, there is an increasing role that cyber infrastructures will play in existing control systems and in domains as diverse as the process control industry, the power grid, oil and natural gas infrastructure, autonomous vehicle and transportation systems, and medical devices and systems.

Many CPS applications are safety-critical: their failure can cause irreparable harm to the physical system under control and to the people who depend on it. In particular, the protection of our critical infrastructures that rely on CPS, such as the electric power transmission and distribution, industrial control systems, oil and natural gas systems, water and waste-water treatment plants, healthcare devices, and transportation networks play a fundamental and large-scale role in our society—and their disruption can have a significant impact to individuals, and nations at large.

Similarly, because many CPS systems collect sensor data non-intrusively, users of these systems are often unaware of their exposure. Therefore in addition to security, CPS systems must be designed with privacy considerations.

The challenges in securing CPS are many. But fundamentally, it is important to recognize that securing CPS differs from the traditional cyber security concerns of confidentiality, integrity and availability (CIA) that have dominated the security of information technology (IT) systems. At its core, CPS security must be approached and framed from the perspective of how attacks on CIA properties perturb control-theoretic properties such as controllability, observability and stability, and in turn the impact on overall system reliability and safety.

## 2. OBJECTIVE AND SCOPE

The objective and vision of the workshop is that it becomes the premiere forum to publish research on CPS security and privacy. As such the second edition of this workshop builds on vision set by the first workshop and invited participation from diverse CPS domains, researchers and practitioners, and encompassed a range of topics. Submissions were sought from multiple interdisciplinary backgrounds representative of CPS, including but not limited to information security, control theory, embedded systems, and human factors. In particular, the workshop sought contributions in the following topic areas:

- mathematical foundations for secure CPS
- control theoretic approaches to secure CPS
- security architectures for CPS

*CCS'16 October 24-28, 2016, Vienna, Austria*

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2990481

- security and resilience metrics for CPS
- metrics and risk assessment approaches for CPS
- privacy in CPS
- network security for CPS
- game theory applied to CPS security
- security of embedded systems, IoT and real-time systems in the context of CPS
- human factors and humans in the loop
- CPS reliability and safety
- economics of security and privacy in CPS
- intrusion detection in CPS

CPS domains of interest included but are not limited to:

- health care and medical devices
- manufacturing
- industrial control systems
- SCADA systems
- robotics
- unmanned aerial vehicles (UAVs)
- autonomous vehicles
- transportation systems and networks
- abstract theoretical CPS domains that involve sensing and actuation

## 3. PROGRAM COMMITTEE

We are thankful to the members of our program committee without whose help and support this workshop wouldn't have been possible.

- Gail-Joon Ahn, Arizona State Univ., USA
- Christina Alcaraz, University of Malaga, Spain
- Magnus Almgren, Chalmers Univ., Sweden
- Pauline Anthonysamy, Google
- Robin Berthier, UIUC, USA
- Raheem Beyah, Georgia Tech., USA
- Binbin Chen, ADSC, Singapore
- Richard Chow, Intel, USA
- Gyorgy Dan, KTH, Sweden
- Bela Genge, Petru Maior Univ., Romania
- Ryan Gerdes, Utah State Univ., USA
- Dieter Gollman, TU Hamburg, Germany
- Adam Hahn, Washington State Univ., USA
- Jun Ho Huh, Honeywell ACS Labs, USA
- Jorjeta Jetcheva, Fujitsu Lab, USA
- Xenofon Koutsoukos, Vanderbilt Univ., USA
- Marina Krotofil, Honeywell ICS Lab, USA
- Deepa Kundur, Univ. of Toronto, Canada
- Michail Maniatakos, NYU-Abu Dhabi, UAE
- Jonathan Marguiles, Qmulos, USA
- Daisuke Mashima, ADSC, Singapore
- Aditya Mathur, SUTD, Singaopore
- Stephen McLaughlin, Google, USA
- Sibin Mohan, UIUC, USA
- Xinming Ou, Univ. of South Florida, USA
- Marina Papatriantafilou, Chalmers Univ., Sweden
- Siva Rajagopalan, Honeywell ACS Labs, USA
- Awais Rashid, Lancaster Univ., UK
- Lillian Ratliff, Univ. of Washington, USA
- Billy Rios, WhiteScope, USA
- Sandra Rueda, Univ. of the Andes, Columbia
- Justin Ruths, UT Dallas, USA
- Henrik Sandberg, KTH, Sweden
- Sean Smith, Dartmouth, USA
- Rui Tan, ADSC, Singapore
- Roshan Thomas, MITRE, USA
- Selcuk Uluagac, Florida International Univ., USA
- Alfonso Valdes, UIUC, USA
- Claire Vishik, Intel, USA
- Avishai Wool, Tel Aviv Univ., Israel
- Mark Yampolskiy, Univ. of South Alabama, USA
- Attila Yavuz, Oregon State Univ., USA
- Jianying Zhou, Inst. for Infocomm Research, Singapore
- Quanyan Zhu, NYU, USA
- Saman Zonouz, Rutgers Univ., USA

## 4. PC CO-CHAIRS

**Alvaro A. Cárdenas** is an Assistant Professor at the Department of Computer Science at the University of Texas at Dallas. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park. Before joining UT Dallas he was a postdoctoral scholar at the University of California, Berkeley, and a research staff at Fujitsu Laboratories of America in Sunnyvale California. His research interests focus on computer security, cyber-physical systems, network intrusion detection, and wireless networks. He is the recipient of the NSF CAREER award, best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Office, and a Graduate School Fellowship from the University of Maryland. Together with Roshan K. Thomas and Rakesh B. Bobba he initiated CPS-SPC 2015.

**Rakesh B. Bobba** is an Assistant Professor in the School of Electrical Engineering and Computer Science (EECS) at Oregon State University (OSU). He obtained his Ph.D. and M.S. in Electrical and Computer Engineering from the University of Maryland at College Park. Prior to joining OSU, Dr. Bobba was a Research Assistant Professor at the Information Trust Institute, University of Illinois, Urbana-Champaign. His research interests are in the design of secure and trustworthy networked and distributed computer systems, with a current focus on cyber-physical critical infrastructures, shared computing infrastructures and real-time systems. Together with Roshan K. Thomas and Alvaro C. Cardenas he initiated CPS-SPC 2015.